Kasra Ahmadi, Ph.D Candidate.

Work Authorization: U.S. Permanent Residency Process Initiated (Approved I-140 (NIW))
Tampa, FL, 33617 | kasra.research@gmail.com | 8136142640 | https://kasraahmadi.github.io/
LinkedIn: https://www.linkedin.com/in/kasra-ahmadii | GitHub: https://github.com/KasraAhmadi | Google Scholar

Education

- **Ph.D. in Computer Science** - *University of South Florida, Tampa* **-** Jan 2022 to Dec 2025.
  Focus: Privacy in ML and Post-Quantum Cryptography | Advisor: Prof. Mehran Mozaffari Kermani | GPA: 3.93/4
- **M.Sc. in Information Technology** - *Amirkabir University of Technology, Tehran* - Sep 2018 to Sep 2021.
  Focus: Secure file sharing market on Blockchain using smart contracts [C.1]
- **B.Sc. in Computer Science -** *Isfahan University of Technology, Isfahan* - Sep 2012 to Jul 2017.

Work Experience

- **Graduate Research Assistant -** *University of South Florida, Tampa, FL* Jan 2022 - present
  - **Privacy in Machine Learning** [S.1]: Developed an innovative framework that integrates differential privacy and federated learning for fine-tuning large language models (LLMs), optimizing memory usage on resource-constrained devices while maintaining high model accuracy. https://github.com/KasraAhmadi/FL-Privacy-LLM
  - **Post-Quantum Cryptography:**
    - Designed, simulated, and implemented algorithm level error detection schemes for NTT module used for fast polynomial multiplication in Kyber and Dilithium to mitigate fault attacks, assessed on FPGAs and ARM microcontrollers [S.2, S.5].
    - Improve Kyber and Dilithium in speed by using PUF to generate random numbers [J.1, J.4].
  - **Fault Detection on Classical Cryptography** [J.2, J.3, S.3, S.4, S.5]:
    - Developed, simulated, and deployed algorithm-level error detection schemes for the Montgomery multiplication algorithm in the Elliptic Curve Scalar Multiplication (ECSM) module to mitigate fault attacks, evaluated on FPGAs and ARM microcontrollers.
  - Work under National Science Foundation (NSF) Grant #1801488.
  - Teaching assistant of graduated Cryptography, Operating Systems, Network Lab, and System Design Lab.

- **Software Engineer Intern** - *Agwise, St.Petersburg, FL* May 2024 - Aug 2024
  - Led the technical team in designing and implementing an event-driven architecture using AWS services to develop a recommender system for nutrient optimization in high-yield corn and soybean farming.
  - Developed an ETL pipeline using AWS Lambda and AWS Glue to extract nutrient data from labs, store it in a data lake (S3), and apply recommendation algorithms and load it into database.
  - Improved existed frontend and backend services performance by 30% through optimization techniques and caching strategies.

- **Machine Learning Engineer,** *Paar Lift, Tehran* Jan 2019 - Apr 2020

  Worked in an elevator manufacturing company to implement machine learning on elevator control boards. Optimized elevator operations, reducing hotel guests' wait times by 27%, saving an average of 11 seconds per passenger per day.
  - **Machine Learning:**
    - Developed an elevator simulation engine using Python to analyze optimal floor assignments at different times, aiming to minimize passenger wait times using machine learning techniques like Neural Networks and KNN.
    - After validating the approach through simulations, we transitioned to real-world implementation with designing ETL pipelines using Apache Airflow to extract, ingest, and load elevator traffic data into a data warehouse.
  - **Software Engineering:**
    - Implemented and maintained reliable real-time gateway module for Raspberry pi to capture elevator moving data via CAN bus protocol and transmits that data to server using websocket.

Skills

Software	Python, C++, Typescript, Node.js, Java, JavaScript, QT
Embedded	Vivado, Vitis, ARM, FPGA, HLS
Cloud	AWS, GCP
Databases	SQL, MongoDB
Other	Git, Docker
Soft-skills	Analytical Thinking, Problem-Solving, Goal Alignment, Communication, Adaptability

Publications

C=Conference, J=Journal, S=In Submission

[S.1] Ahmadi, K, et al (2025), "An Interactive Framework for Implementing Privacy-Preserving Federated Learning: Experiments on Large Language Model." Manuscript submitted to *IEEE Symposium on Security and Privacy 2025*

[J.1] Aghapour, S., Ahmadi, K., Anastasova, M, et al. (2025). "PUF-Dilithium: Design of a PUF-Based Dilithium Architecture Benchmarked on ARM Processors." *ACM Trans. Embed. Comput. Syst., 24(2).*

[J.2] Ahmadi, K., et al. (2024). "Efficient Error Detection Schemes for ECSM Window Method Benchmarked on FPGAs." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 32(3), 592-596.*

[J.3] Ahmadi, K., et al. (2024). "Efficient Error Detection Cryptographic Architectures Benchmarked on FPGAs for Montgomery Ladder." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 32(11), 2154-2158.*

[J.4] Aghapour, S., Ahmadi, K., Anastasova, M, et al. (2024). "PUF-Kyber: Design of a PUF-Based Kyber Architecture Benchmarked on Diverse ARM Processors." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 43(12), 4453-4462.*

[C.1] Ahmadi, K. et al. (2023). "A P2P file sharing market based on blockchain and ipfs with dispute resolution mechanism." *In 2023 IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings) (pp. 1-5).*

[S.2] Ahmadi, K, et al (2025), "Efficient Algorithm Level Error Detection for Number-Theoretic Transform Assessed on FPGAs and ARM" Manuscript submitted to *ACM Trans. Embed. Comput. Syst.*

[S.3] Ahmadi, K, et al (2025), "Error Detection Schemes for τ-NAF Conversion within Koblitz Curves Benchmarked on Various ARM Processors" Manuscript submitted to *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.*

[S.4] Aghapour, S., Ahmadi, K., Kermani, M, et al (2024) "Efficient Fault Detection Architectures for Modular Exponentiation Targeting Cryptographic Applications Benchmarked on FPGAs" Manuscript submitted to *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems II.*

[S.5] Darzi, S., Ahmadi, K., Aghapouri, S, et al (2023) "Envisioning the future of cyber security in post-quantum era: A survey on pq standardization, applications, challenges and opportunities" Manuscript submitted to *ACM Comp Survey.*

Certifications

- AWS Certified Solutions Architect - Associate, View Certification (Dec 2023)
- Deep Neural Networks with PyTorch, View Certificate (Oct 2024)
- Intro to Federated Learning, View Certificate (Oct 2024)
- Artificial Intelligence Privacy and Convenience, View Certificate (Aug 2024)
- Federated Fine-tuning of LLMs with Private Data, View Certificate (Aug 2024)
- ETL and Data Pipelines with Shell, Airflow and Kafka, View Certificate (Jan 2024)
- Divide and Conquer, Sorting and Searching, and Randomized Algorithms, View Certificate (Oct 2023)

Services

- Mentor at REU Site: Cryptography and Coding Theory at the University of South Florida (Summer, 2023) NSF award: 2244488
- Conducted peer review for **17** manuscripts from "Transactions on Embedded Computing Systems", "IEEE Transactions on Circuits and Systems I: Regular Papers", and "IEEE Transactions on Very Large Scale Integration (VLSI) Systems".